

Nonexistence of twenty-fourth power residue addition sets

Ron Evans
Department of Mathematics
University of California at San Diego
La Jolla, CA 92093-0112
revans@ucsd.edu

and

Mark Van Veen
Varasco LLC
2138 Edinburg Avenue
Cardiff by the Sea, CA 92007
mark@varasco.com

November 2016

2010 *Mathematics Subject Classification*. 05B10, 11T22, 11T24, 15A06.

Key words and phrases. power residues, difference sets, qualified difference sets, Jacobi sums, cyclotomic numbers

Abstract

Let $n > 1$ be an integer, and let \mathbb{F}_p denote a field of p elements for a prime $p \equiv 1 \pmod{n}$. By 2015, the question of existence or nonexistence of n -th power residue difference sets in \mathbb{F}_p had been settled for all $n < 24$. We settle the case $n = 24$ by proving the nonexistence of 24-th power residue difference sets in \mathbb{F}_p . We also prove the nonexistence of *qualified* 24-th power residue difference sets in \mathbb{F}_p . The proofs make use of a Mathematica program which computes formulas for the cyclotomic numbers of order 24 in terms of parameters occurring in quadratic partitions of p .

1 Introduction

For an integer $n > 1$, let p be a prime of the form $p = nf + 1$. Let H_n denote the set of nonzero n -th power residues in \mathbb{F}_p , where \mathbb{F}_p is the field of p elements. For $\epsilon \in \{0, 1\}$, define $H_{n,\epsilon} = H_n \cup \{1 - \epsilon\}$. Note that the set $H_{n,\epsilon}$ has $f + \epsilon$ elements.

Fix $m \in \mathbb{F}_p^*$. Lam [12] called $H_{n,\epsilon}$ an n -th power residue addition set if the list of differences $s - mt \in \mathbb{F}_p^*$ with $s, t \in H_{n,\epsilon}$ hits each element of \mathbb{F}_p^* the same number of times. If m is an n -th power residue, such an addition set is called an n -th power residue difference set. If m is not an n -th power residue, then as in [3, p. 94], such an addition set is called a qualified n -th power residue difference set with qualifier m .

Let g denote a primitive root modulo p . For integers s, t modulo n , the cyclotomic number $C_n(s, t)$ of order n is defined to be the number of integers $N \in \mathbb{F}_p$ for which both N/g^s and $(N+1)/g^t$ are nonzero n -th power residues in \mathbb{F}_p . If $H_{n,\epsilon}$ is a difference set, then necessarily [9, p. 677] n is even, f is odd, and

$$(1.1) \quad n^2 C_n(s, 0) = p - 1 + 2n\epsilon - n, \quad 1 \leq s < n/2.$$

If $H_{n,\epsilon}$ is a qualified difference set, then necessarily [3, Theorems 2.1 and 2.2] n is even, f is even, and

$$(1.2) \quad n^2 C_n(s, n/2) = p - 1 + 2n\epsilon, \quad 1 \leq s < n/2.$$

For $n < 24$, it is known that $H_{n,\epsilon}$ can be a difference set only in the three exceptional cases $H_{2,\epsilon}$, $H_{4,\epsilon}$, $H_{8,\epsilon}$ listed in [3, (1.1)–(1.3)]. This follows

from the work of a number of different authors during the period 1933–2015. For references, consult Xia [13], who has extended the results to fields of q elements, where q is a prime power. In Section 4, we prove that $H_{24,\epsilon}$ cannot be a difference set, by showing that (1.1) cannot hold for $n = 24$.

For $n < 22$, it is known that $H_{n,\epsilon}$ can be a qualified difference set only in the three exceptional cases $H_{2,\epsilon}$, $H_{4,\epsilon}$, $H_{6,\epsilon}$ listed in [3, (1.4)–(1.6)]. In Section 3, we prove that $H_{24,\epsilon}$ cannot be a qualified difference set, by showing that (1.2) cannot hold for $n = 24$.

Our proofs depend on formulas for the cyclotomic numbers $C_{24}(s, t)$. Printed tables of these formulas were archived in 1979 [8], but it is much more useful to have digital access. Thus we wrote a Mathematica program [10] to compute the formulas for $C_{24}(s, t)$. This program is described in the next section.

We remark that besides their use for analyzing power residue difference sets, cyclotomic numbers have applications to such topics as counting points on elliptic curves [14], Gauss periods and complexity of normal bases for finite fields [4],[11], cyclic codes [6], cryptographic functions [5], residuacity [1, Chapter 7], linear complexity of sequences [2], and almost difference sets [7].

2 Cyclotomic numbers of order 24

Let $\beta = \exp(2\pi i/24)$. For $0 \leq u, v \leq 23$, define the Jacobi sum $J(u, v, \beta)$ by

$$(2.1) \quad J(u, v) = J(u, v, \beta) = \sum_{x=2}^{p-1} \beta^{\text{ind}(x)u + \text{ind}(1-x)v},$$

where $\text{ind}(x)$ denotes the index of x with respect to the primitive root g . The cyclotomic numbers $C_{24}(s, t)$ can be computed in terms of Jacobi sums via the formula [1, eq. 2.5.1]

$$(2.2) \quad 576C_{24}(s, t) = \sum_{u=0}^{23} \sum_{v=0}^{23} (-1)^{uf} \beta^{-su-tv} J(u, v, \beta).$$

There are five Jacobi sums in (2.2) that have been expressed in [9, p. 678] in terms of sixteen integer parameters called

$$(2.3) \quad X, Y, A, B, C, D, U, V, D_j, \quad 0 \leq j \leq 7,$$

viz.

$$(2.4) \quad J(6, 12) = -X + 2Yi, \quad (p = X^2 + 4Y^2, \quad X \equiv 1 \pmod{4}),$$

$$(2.5) \quad J(4, 12) = -A + Bi\sqrt{3}, \quad (p = A^2 + 3B^2, \quad A \equiv 1 \pmod{6}),$$

$$(2.6) \quad J(3, 12) = -C + Di\sqrt{2}, \quad (p = C^2 + 2D^2, \quad C \equiv 1 \pmod{4}),$$

$$(2.7) \quad J(1, 12) = U + 2Vi\sqrt{6}, \quad (p = U^2 + 24V^2, \quad U \equiv -C \pmod{3}),$$

$$(2.8) \quad J(1, 2) = \sum_{j=0}^7 D_j \beta^j.$$

The remaining Jacobi sums in (2.2) are expressible [1, Chapter 3] in terms of the parameters (2.3) together with the four parameters

$$(2.9) \quad F1, V1, Z, T,$$

where $F1 \in \{0, 1\}$ with $F1 \equiv f \pmod{2}$, $V1 \in \{0, 1\}$ with $V1 \equiv V \pmod{2}$, $Z \equiv \text{ind}(2) \pmod{12}$, and $T \equiv \text{ind}(3) \pmod{8}$. As described in [9, p. 678], g may be chosen so that $Z \in \{0, 2, 4, 6\}$ and $T \in \{0, 2, 4\}$. Thus there are 48 distinct 4-tuples $\{F1, V1, Z, T\}$, and for each such 4-tuple, one can create a table of the 576 numbers

$$(2.10) \quad 576C_{24}(s, t), \quad 0 \leq s, t \leq 23.$$

Each number in (2.10) turns out to be an integer linear combination of

$$(2.11) \quad p, 1, X, Y, A, B, C, D, U, V, D_0, D_1, D_2, D_3, D_4, D_5, D_6, D_7.$$

For example, when $\{F1, V1, Z, T\} = \{1, 1, 4, 0\}$, we have

$$(2.12) \quad \begin{aligned} 576C_{24}(6, 0) = & p - 23 + 4X + 0Y - 14A + 24B - 8C + 0D - 8U \\ & + 0V + 32D_0 + 0D_1 + 0D_2 + 0D_3 + 16D_4 + 0D_5 + 0D_6 + 0D_7. \end{aligned}$$

Our Mathematica module `CycFull[s, t, F1, V1, Z, T]` in [10] outputs a list beginning with s, t followed in order by the coefficients in the linear combination of the elements in (2.11). For example, in view of (2.12), the input `CycFull[6, 0, 1, 1, 4, 0]` outputs the list

$$\{6, 0, 1, -23, 4, 0, -14, 24, -8, 0, -8, 0, 32, 0, 0, 0, 16, 0, 0, 0\}.$$

For each of the 48 tuples $\{F1, V1, Z, T\}$, CycFull can be used to construct a table of the 576 cyclotomic numbers of order 24.

We now describe two additional Mathematica modules, CycShort6 and CycShort8, which will be used in the sequel. CycShort6 is like CycFull except that the output list is shortened by omitting the first four entries and also omitting the coefficients of the six parameters D, V, D_1, D_3, D_5, D_7 . CycShort8 is like CycShort6 except that the output list is further shortened by omitting the coefficients of the two parameters D_2, D_6 . For example, CycShort6[6, 0, 1, 1, 4, 0] outputs the list

$$\{4, 0, -14, 24, -8, -8, 32, 0, 16, 0\}$$

of coefficients of

$$(2.13) \quad X, Y, A, B, C, U, D_0, D_2, D_4, D_6,$$

while CycShort8[6, 0, 1, 1, 4, 0] outputs the list

$$\{4, 0, -14, 24, -8, -8, 32, 16\}$$

of coefficients of

$$(2.14) \quad X, Y, A, B, C, U, D_0, D_4.$$

3 Nonexistence of qualified difference sets

In this section we focus on the 24 tuples $\{0, V1, Z, T\}$, which correspond to Tables 1–24 in [10]. Running CycFull[$s, 12, 0, V1, Z, T$], we see that

$$(3.1) \quad 576C_{24}(s, 12) = p + 1 + \gamma_0(s), \quad 1 \leq s \leq 11,$$

where

$$\gamma_0(s) = d_1X + d_2Y + d_3A + d_4B + d_5C + d_6U + d_7D_0 + d_8D_2 + d_9D_4 + d_{10}D_6$$

for integer coefficients d_j depending on $s, V1, Z, T$. Thus the coefficients of $\gamma_0(s)$ are given by CycShort6[$s, 12, 0, V1, Z, T$]. Moreover, in the eight cases where $T = 4$, the coefficients d_8 and d_{10} are always 0, so in those eight cases, the coefficients of $\gamma_0(s)$ are given by CycShort8[$s, 12, 0, V1, Z, T$].

Assume for the purpose of contradiction that (1.2) holds. Then by (3.1), we have the following system of eleven linear equations:

$$(3.2) \quad \gamma_0(s) = -2 + 48\epsilon, \quad 1 \leq s \leq 11.$$

We will prove that the system (3.2) has no viable solution, thus obtaining the desired result that (1.2) cannot hold.

The system (3.2) can be represented as a matrix equation of the form

$$(3.3) \quad M\mathbf{y} = \mathbf{h},$$

where M is an 11 by 10 matrix of integer coefficients, \mathbf{y} is the column vector whose ten entries are the variables in (2.13), and \mathbf{h} is the column vector whose eleven entries all equal $-2 + 48\epsilon$. In the eight cases where $T = 4$, we can instead take M as an 11 by 8 matrix of integer coefficients with \mathbf{y} the column vector whose eight entries are the variables in (2.14). Our matrix equations are displayed in [10] in Tables 1–24. In several cases, our matrix equations don't need to make use of all eleven rows of the matrix M . For example, for Table 21, we obtain a contradiction with a coefficient matrix consisting only of rows 4 through 11, i.e., the top three rows of M have been omitted.

For each of the 24 tables, a particular solution to the matrix equation is found using the Mathematica function `LinearSolve`. To find the general solution, we add the particular solution to the null space of the matrix, computed in the tables with the function `NullSpace`. We proceed to examine the general solutions table by table, and show that none of them are viable.

Table 1

As shown in [10], in the general solution to the matrix equation, we have

$$X = A = 1 - 24\epsilon, \quad B = 2b, \quad D_0 = -1 + 24\epsilon - b$$

for some b , and b must be an integer since D_0 is. By the formulas for p in (2.4)–(2.5), we have $4Y^2 = 12b^2$. This contradicts the fact that 3 is not a square, so the matrix equation has no viable solution.

Tables 2,3,7,9,10,11,12,13,14,15,23,24

In the general solution, $B = 0$, which contradicts (2.5).

Tables 4,5,6,16,17,18,19,20,21

In the general solution, X is not an integer, which is a contradiction.

Table 8

In the general solution,

$$X = 1 - 24\epsilon - 16a, \quad Y = a, \quad A = -1 + 24\epsilon + 8a, \quad B = -4a$$

for some a , and a must be a nonzero integer since Y is. By the formulas for p in (2.4)–(2.5), we have

$$p = (1 - 24\epsilon - 16a)^2 + 4a^2 = (-1 + 24\epsilon + 8a)^2 + 48a^2.$$

Solving for a yields $a = (4 - 96\epsilon)/37$, which contradicts the fact that a is an integer.

Table 22

In the general solution, for some a , we have

$$X = (-1 + 24\epsilon)/23 + 192a, \quad Y = 92a, \quad A = 9(-1 + 24\epsilon)/23 + 256a, \quad B = 138a.$$

By the formulas for p in (2.4)–(2.5), we have

$$((-1 + 24\epsilon)/23 + 192a)^2 + 4(92a)^2 = (9(-1 + 24\epsilon)/23 + 256a)^2 + 3(138a)^2.$$

Solving for a yields $a = (2 - 48\epsilon)/897$ or $a = (10 - 240\epsilon)/7659$. In particular, $46a$ is not an integer. However, in the general solution, we also have $46a = D_7 - D_6$, which is not possible since D_7 and D_6 are integers.

This completes the proof that $H_{24,\epsilon}$ cannot be a qualified difference set.

4 Nonexistence of difference sets

In this section we focus on the 24 tuples $\{1, V1, Z, T\}$, which correspond to Tables 25–48 in [10]. Running $\text{CycFull}[s, 0, 1, V1, Z, T]$, we see that

$$(4.1) \quad 576C_{24}(s, 0) = p - 23 + \gamma_1(s), \quad 1 \leq s \leq 11,$$

where

$\gamma_1(s) = c_1X + c_2Y + c_3A + c_4B + c_5C + c_6U + c_7D_0 + c_8D_2 + c_9D_4 + c_{10}D_6$ for integer coefficients c_j depending on $s, V1, Z, T$. Thus the coefficients of $\gamma_1(s)$ are given by `CycShort6`[$s, 0, 1, V1, Z, T$]. Moreover, in the eight cases where $T = 0$, the coefficients c_8 and c_{10} are always 0, so in those eight cases, the coefficients of $\gamma_1(s)$ are given by `CycShort8`[$s, 0, 1, V1, Z, T$].

Assume for the purpose of contradiction that (1.1) holds. Then by (4.1), we have the following system of eleven linear equations:

$$(4.2) \quad \gamma_1(s) = -2 + 48\epsilon, \quad 1 \leq s \leq 11.$$

In the same manner used in the previous section, we will prove that the system (4.2) has no viable solution, thus obtaining the desired result that (1.1) cannot hold.

Tables 25,26,27,28,30,31,33,34,36,38,39,47,48

In the general solution, we have $B = 0$ or $Y = 0$, both of which are impossible.

Tables 29,32,35,41,42,43,44,45,46

In the general solution, X is not an integer, which is a contradiction.

Table 37

In the general solution,

$$X = 5 - 120\epsilon, \quad A = 13 - 312\epsilon, \quad C = -23 + 552\epsilon, \quad U = -1 + 24\epsilon$$

and for some a ,

$$B = -2a, \quad D_0 = 8 - 192\epsilon - a, \quad D_4 = 2a.$$

Here a must be a nonzero integer since D_0 is an integer and B is nonzero. We do not see how to obtain a contradiction via the systematic method used for the other tables. However, a contradiction has been obtained using Gauss sums of order 24; see [9, pp. 680–683]. (*Note:* On lines 22, 26, 30, 32 of [9, p. 680], subtract 7 from each reference number. Also, on line 2 of the Introduction in [9], replace the second p by e .)

Table 40

In the general solution, for some a ,

$$\begin{aligned} X &= (-5 + 120\epsilon)/19 - 24a, \quad Y = -19a, \\ A &= (-17 + 408\epsilon)/19 - 112a, \quad B = (7 - 168\epsilon)/19 + 26a. \end{aligned}$$

Here $19a$ is an integer, since Y is. By the formulas for p in (2.4)–(2.5), we have

$$\begin{aligned} &((-5 + 120\epsilon)/19 - 24a)^2 + 1444a^2 = \\ &((-17 + 408\epsilon)/19 - 112a)^2 + 3((7 - 168\epsilon)/19 + 26a)^2. \end{aligned}$$

This equation has irrational solutions a , which is a contradiction.

This completes the proof that $H_{24,\epsilon}$ cannot be a difference set.

References

- [1] B. C. Berndt, R. J. Evans, and K. S. Williams, Gauss and Jacobi sums, Wiley–Interscience, New York, 1998.
- [2] N. Brandstätter and A. Winterhof, Subsequences of Sidelnikov sequences, Contemp. Math. 461 (2008), 33–45.
- [3] K. Byard, R. Evans and M. Van Veen, Lam’s power residue addition sets, Advances in Applied Mathematics 46 (2011), 94–108.
- [4] M. Christopoulou, T. Garefalakis, D. Panario, and D. Thomson, Gauss periods as constructions of low complexity normal bases, Des. Codes Cryptogr. 62 (2012), no. 1, 43–62.
- [5] T. Cusick, C. Ding, and A. Renvall, Stream Ciphers and Number Theory. Revised ed., Amsterdam: North-Holland Mathematical Library, Elsevier Science B.V., 2004, vol. 66.
- [6] C. Ding, A class of three-weight and four-weight codes, Coding and cryptology, pp. 34–42, Lecture Notes in Comput. Sci., 5557, Springer, Berlin, 2009.
- [7] C. Ding, A. Pott, and Q. Wang, Constructions of almost difference sets from finite fields, Des. Codes Cryptogr. 72 (2014), 581–592.

- [8] R. Evans, Table of cyclotomic numbers of order twenty-four, *Math. Comp.* 35 (1980), 1036–1038; UMT file 12[9.10], 98 pp.
- [9] R. Evans, Twenty-fourth power residue difference sets. *Math. Comp.* 40 (1983), 677–683.
- [10] R. Evans and M. Van Veen, Cyclotomic numbers of order 24, Mathematica program,
<http://www.math.ucsd.edu/~revans/Cyc24.nb>
<http://www.math.ucsd.edu/~revans/Cyc24.pdf>
- [11] S. Gao and D. Thomson, Complexity of normal bases, *Handbook of Finite Fields*, Gary Mullen and Daniel Panario, editors, pp. 117–128, CRC Press, Boca Raton, FL, 2013.
- [12] C. Lam, Nth power residue addition sets, *J. Combin. Theory Ser. A* 20 (1976), 20–33.
- [13] B. Xia, Cyclotomic difference sets in finite fields, arXiv:1501.03275
- [14] L. Xia and J. Yang, Cyclotomic problem, Gauss sums and Legendre curve, *Sci. China Math.* 56 (2013), no. 7, 1485–1508.